# The MITNET external access facility (DISA) and its authorization codes

## 1. RESPONSIBILITIES

1.1 Implementation of this policy at missions is the responsibility of the Head of Mission through the mission Administration staff. The Mission Security Officer is to assure, together with the mission or regional technician (EL), that proper restrictions are applied.

1.2 Implementation of this policy at Headquarters is the responsibility of the Director of the Telecommunications Division (MST) through appropriate MST delegated administration staff.

## 2. DIRECT INWARD SYSTEM ACCESS (DISA)

Direct Inward System Access (DISA) is a powerful feature which permits a caller on the local commercial exchange to dial directly into a private telephone system (mission or Headquarters) without attendant assistance to gain access to telephone facilities.

### 2.1 Restrictions

2.1.1 DISA enables an authorized individual to access the department's telephone network and be recognized as a user. Adequate controls must be applied to prevent costly unauthorized use on this expensive network.

2.1.2 Guarding your authorization code is of utmost importance. It is proven that passwords or authorization codes are not effective control measures unless properly handled. The ease with which "hackers" can penetrate networks is well documented and presents substantial risks if the access is not well controlled. Technology available to hackers allows them to pierce through barriers made of codes which are not properly set up and administered, by using commonly available PCs and modems. Booklets are available on the market where DISA numbers are sold at a minimal price for buyers to gain access to a corporation's system to make long distance calls at that corporation's expense.

# Le dispositif d'accès externe du MITNET (ADAS) et ses codes d'accès

## 1. RESPONSABILITÉS

1.1 À la mission, il incombe au chef de mission d'assurer la mise en oeuvre de la présente politique, par l'entremise du personnel administratif de la mission. L'agent de sécurité de la mission doit, avec l'aide du technicien rattaché à la mission ou du technicien régional (EL), veiller à l'application des restrictions appropriées.

1.2 À la Centrale, il incombe au directeur de la Direction des télécommunications (MST) d'assurer la mise en oeuvre de la présente politique, par l'entremise du personnel administratif délégué approprié.

## 2. ACCÈS DIRECT AU SYSTÈME (ADAS)

L'Accès direct au système (ADAS) est un dispositif qui permet à une personne composant un appel à partir d'un centre local, rattaché à un réseau commercial, d'accéder directement à un système téléphonique privé (celui d'une mission ou de l'Administration centrale), sans l'aide d'un préposé.

### 2.1 Restrictions

2.1.1 L'ADAS permet à une personne autorisée d'accéder au réseau du Ministère et d'être reconnue comme usager autorisé. On doit donc mettre en place des mécanismes aptes à empêcher tout usage non autorisé et coûteux de ce réseau dispendieux.

2.1.2 Il est prouvé que les mots de passe et les codes d'autorisation ne constituent pas des mesures de contrôle efficaces s'ils ne sont pas bien administrés, et il existe une importante documentation sur la facilité avec laquelle des «intrus» peuvent s'introduire dans des réseaux dont l'accès est insuffisamment contrôlé. La technologie accessible aux intrus leur permet, au moyen d'ordinateurs personnels et de modems courants, de faire échec aux obstacles composés de codes si ces derniers sont mal établis et mal administrés. On sait que pour des sommes modestes, il est possible de se procurer sur le marché des dépliants dévoilant les numéros ADAS donnant accès aux systèmes d'un organisme ou permettant d'effectuer des appels interurbains aux frais de cet organisme. Il est donc de la plus haute importance que les utilisateurs protègent adéquatement leur code d'autorisation.